



Patent
Attorney's Docket No. 032326-128

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)
David NACCACHE et al) Group Art Unit: 2171
Application No.: 09/802,968) Examiner: Unassigned
Filed: March 12, 2001)
For: A PROBABILISTIC DIGITAL)
SIGNATURE METHOD)

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:


French Patent Application No. 0003918,
Filed: March 28, 2000.

In support of this claim, enclosed is a certified copy of the prior foreign application. This application is referred to in the oath or declaration. Acknowledgment of receipt of this certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: July 23, 2001

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

This Page Blank (uspto)



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **20 MARS 2001**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

**INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE**

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
<http://www.inpi.fr>

THIS PAGE BLANK (USPTO)

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 w / 260899

REMISE DES PIÈCES DATE 28 MARS 2000 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0003918 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 28 MARS 2000		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE Cabinet BALLOT-SCHMIT 16, Avenue du Pont Royal 94230 CACHAN FRANCE MK/PL	
Vos références pour ce dossier <i>(facultatif)</i> 015519 (GEM851)			
Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> N° / / <i>ou demande de certificat d'utilité initiale</i> N° / /			
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/> N° / /	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé de signatures numériques probabilistes.			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date / / N° Pays ou organisation Date / / N° Pays ou organisation Date / / N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		GEMPLUS	
Prénoms			
Forme juridique		(Société Anonyme)	
N° SIREN			
Code APE-NAF			
Adresse	Rue	Avenue du Pic de Bertagne Parc d'Activités de la Plaine de Jouques	
	Code postal et ville	13420 GEMENOS	
Pays		FRANCE	
Nationalité		Française	
N° de téléphone <i>(facultatif)</i>			
N° de télécopie <i>(facultatif)</i>			
Adresse électronique <i>(facultatif)</i>			

REMISE DES PIÈCES DATE 28 MARS 2000 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0003918 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	08 540 W / 260899
Vos références pour ce dossier : (facultatif)		015519 (GEM851)	
6 MANDATAIRE			
Nom		BORIN	
Prénom		Lydie	
Cabinet ou Société		Cabinet BALLOT-SCHMIT	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	16, Avenue du Pont Royal	
	Code postal et ville	94230 CACHAN	
N° de téléphone (facultatif)		01 49 69 91 91	
N° de télécopie (facultatif)		01 49 69 91 90	
Adresse électronique (facultatif)			
7 INVENTEUR (S)			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en deux versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Lydie BORIN Mandataire N° 94-0506 Cabinet BALLOT-SCHMIT		VISA DE LA PRÉFECTURE OU DE L'INPI P. BERNOUIS	

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° . 1. / 1..

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		015519 (GEM851)	
N° D'ENREGISTREMENT NATIONAL		0003918	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Procédé de signatures numériques probabilistes.			
LE(S) DEMANDEUR(S) :			
GEMPLUS (S.A.) Avenue du Pic de Bertagne Parc d'Activités de la Plaine de Jouques 13420 GEMENOS FRANCE			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		NACCACHE	
Prénoms		David	
Adresse	Rue	Domicilié au Cabinet BALLOT-SCHMIT 16, Avenue du Pont Royal	
	Code postal et ville	94230	CACHAN
Société d'appartenance (facultatif)			
Nom		PAILLIER	
Prénoms		Pascal	
Adresse	Rue	Domicilié au Cabinet BALLOT-SCHMIT 16, Avenue du Pont Royal	
	Code postal et ville	94230	CACHAN
Société d'appartenance (facultatif)			
Nom		STERN	
Prénoms		Jacques	
Adresse	Rue	Domicilié au Cabinet BALLOT-SCHMIT 16, avenue du Pont Royal	
	Code postal et ville	94230	CACHAN
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)			
Lydie BORIN Mandataire N° 94-0506 Cabinet BALLOT-SCHMIT			

THIS PAGE BLANK (USPTO)

PROCEDE DE SIGNATURES NUMERIQUES PROBABILISTES

La présente invention concerne un procédé de génération de signatures numériques probabilistes afin de permettre la vérification de l'intégrité d'un message transmis.

5 La présente invention s'applique en particulier au domaine des cartes à puce avec ou sans contact. De telles cartes constituent en effet des supports d'informations sécurisés et comportent en général un micro-contôleur incorporé sur une puce de circuit
10 intégré. Un micro-contrôleur possède une architecture semblable à celle d'un ordinateur. Il comporte une unité de traitement constituée d'un microprocesseur ou CPU (de l'anglais Central Processing Unit) associée à différents types de mémoires. Une mémoire non volatile,
15 de type ROM par exemple, comporte en général au moins un programme de mise en œuvre d'un algorithme de signature.

 L'invention s'applique en particulier à des algorithmes de génération et de vérification de
20 signatures numériques. L'objectif de ces algorithmes est de calculer un ou plusieurs entiers, en général une paire, appelés la signature et associés à un message donné afin de certifier l'identité du signataire et l'intégrité du message signé. De tels algorithmes
25 permettent d'une part de générer des signatures et d'autre part de vérifier ces signatures.

 La signature est dite probabiliste lorsque l'algorithme fait appel à un aléas dans la génération de la signature, cet aléas étant secret et régénéré à
30 chaque nouvelle signature. Ainsi, un même message

transmis par un même utilisateur peut avoir plusieurs signatures distinctes.

Un exemple d'un tel algorithme peut être illustré par le DSA (de l'anglais Digital Signature Algorithm).

5 Les paramètres du DSA sont :

- p , un grand premier connu, de 512 ou 1024 bits,
- q , un premier qui divise $p-1$, de 160 bits,
- g , un entier choisi tel que $g^q = 1 \bmod p$
avec $g \neq 1 \bmod p$.

10 La clé secrète x est un nombre aléatoirement fixé entre 0 et $2^{160}-1$, et la clé publique y est liée à x par la relation $y = g^x \bmod p$.

Soit m , le message à envoyer. La signature DSA de m est la paire (r,s) définie comme suit :

15 $r = (g^k \bmod p) \bmod q$;

$s = (h(m) + r \cdot x) / k \bmod q$;

avec k un nombre aléatoire de 160 bits tel que $k < q$, régénéré à chaque signature,

20 et $h(m)$ le message initial m chiffré au moyen d'une fonction de hachage qui est une fonction cryptographique pseudo aléatoire.

La vérification de la signature s'effectue comme suit :

On réalise un premier calcul intermédiaire

25 $w = s^{-1} \bmod q$

On vérifie si $((g^{w \cdot h(m)} y^{r \cdot w}) \bmod p) \bmod q \stackrel{?}{=} r$.

Si cette égalité est vraie, la signature est authentique.

30 La génération de la signature (r,s) a été réalisée avec la clé secrète x et un nombre aléatoire k secret et différent pour chaque signature, et sa vérification avec la clé publique y . Ainsi, n'importe qui peut authentifier une carte et son porteur sans détenir sa clé secrète.

L'utilisation de la fonction de hachage dans la
génération de la signature se retrouve dans quasiment
tous les algorithmes de génération de signatures
probabilistes basés sur un calcul de logarithme
5 discret. Elle permet en effet de garantir la non
reproductibilité de la signature en brisant sa
linéarité.

L'emploi de cette fonction de hachage présente
néanmoins des inconvénients car elle suppose d'une part
10 que cette fonction h se comporte comme une fonction
aléatoire, ce qui n'est pas toujours vrai, et d'autre
part que cette fonction h est implémentée dans la
mémoire de la puce de circuit intégré du dispositif
sécurisé (la carte à puce par exemple). Or la taille de
15 code nécessaire à l'implémentation de la fonction de
hachage est très élevée, environ 1 à 2 kilo octets.

Les contraintes économiques liées au marché de la
carte à puce obligent à une constante recherche en vue
de maîtriser ses coûts de revient. Cet effort passe
20 souvent par l'utilisation de composants plus simples.
Dans un tel cadre, l'implémentation d'algorithmes à clé
publique sur des micro-contrôleurs peu chers de types 8
bits à cœur de 8051 (Intel) ou 6805 (Motorola) par
exemple représente un intérêt grandissant. Il n'est
25 cependant pas possible d'implémenter un algorithme de
signature numérique tel que le DSA ou du même type,
faisant appel à une fonction de hachage, sur de tels
micro-contrôleurs.

L'invention a pour but de résoudre ces contraintes
30 et propose une solution qui soit adaptée à des micro-
contrôleurs possédant peu de ressources de calcul.

La présente invention a pour objet un procédé de
génération de signatures numériques probabilistes qui

permet de s'affranchir de la fonction de hachage, sans altérer la sécurité des messages échangés.

L'invention propose à cet effet un procédé permettant de transformer un algorithme de signature probabiliste utilisant une fonction de hachage en un autre algorithme ne faisant pas appel à cette fonction. A cette fin, l'algorithme probabiliste de départ est utilisé deux fois au lieu d'une pour signer le message directement, c'est à dire le message initial non haché. On génère ainsi des signatures jumelles associées au même message.

L'invention concerne plus particulièrement un procédé de signatures numériques probabilistes d'un message, entre un signataire et un vérifieur, à partir d'un algorithme basé sur le calcul d'un logarithme discret, caractérisé en ce qu'il consiste, pour le signataire, à générer au moins deux signatures du même message non haché, lesdites signatures étant calculées par l'algorithme au moyen des mêmes paramètres à clé publique et privée en faisant respectivement appel à des aléas distincts, et en ce qu'il consiste, pour le vérifieur, à vérifier toutes les signatures dudit message.

Selon une application, l'algorithme probabiliste est le DSA (Digital Signature Algorithm).

Selon une autre application, l'algorithme probabiliste est l'algorithme de Schnorr.

L'invention s'applique avantageusement à tout dispositif sécurisé de type carte à puce, et en particulier à des dispositifs comportant un micro-contrôleur 8 bits.

Le procédé selon l'invention présente l'avantage de s'affranchir de la fonction de hachage et de minimiser ainsi le taux d'occupation mémoire. En outre, la

vitesse de calcul est accrue, même si un double calcul est requis. En effet, l'appel à une fonction de hachage est délicate sur de simples micro-contrôleurs 8 bits, peu chers et de plus en plus souvent utilisés pour
5 contenir les coûts de fabrication des dispositifs.

En outre, le procédé selon l'invention permet de garantir la sécurité dans l'exécution de n'importe quel algorithme de génération de signatures numériques probabilistes.

10 La description fait référence à l'algorithme de signature DSA, mais s'applique également à tous les autres algorithmes de signatures probabilistes et à leurs variantes tels que ElGamal, Schnorr, EC-DSA, Abe-Okamoto, par exemple qui utilisent également la
15 fonction de hachage dans la génération de paires de signatures.

Le procédé de génération de signatures selon l'invention est basé sur le calcul d'au moins deux signatures, que l'on dit alors jumelles, du même
20 message initial m non haché. La signature comprend ainsi au moins deux signatures calculées à l'aide des mêmes paramètres à clé publique y et privée x en faisant respectivement appel à des aléas distincts k_1 , k_2 , ... k_n .

25 La signature du message devient ainsi $(r_1, s_1, r_2, s_2, \dots, r_n, s_n)$, avec les n paires (r_i, s_i) (pour i allant de 1 à n) calculées et vérifiées selon les procédés classiques de génération et de vérification de signatures qu'il s'agisse du DSA, de Schnorr ou de tout autre algorithme
30 utilisant une fonction de hachage.

REVENDICATIONS

1. Procédé de signatures numériques probabilistes d'un message (m), entre un signataire et un vérifieur, à partir d'un algorithme basé sur le calcul d'un logarithme discret, caractérisé en ce qu'il consiste, pour le signataire, à générer au moins deux signatures (r_1, s_1) et (r_2, s_2) du même message non haché (m), lesdites signatures étant calculées par l'algorithme au moyen des mêmes paramètres à clé publique et privée (y, x) en faisant respectivement appel à des aléas distincts (k_1) et (k_2) , et en ce qu'il consiste, pour le vérifieur, à vérifier toutes les signatures (r_1, s_1) et (r_2, s_2) dudit message (m).

2. Procédé selon la revendication 1, caractérisé en ce que l'algorithme probabiliste est le DSA (Digital Signature Algorithm).

3. Procédé selon la revendication 1, caractérisé en ce que, l'algorithme probabiliste est l'algorithme de Schnorr.

4. Dispositif sécurisé, de type carte à puce, caractérisé en ce qu'il comporte un composant électronique apte à mettre en œuvre le procédé de signature selon les revendications 1 à 3.

5. Dispositif selon la revendication 4, caractérisé en ce que le composant électronique est un micro-contrôleur 8 bits.